DEPARTMENT OF HEALTH & HUMAN SERVICES
Centers for Medicare & Medicaid Services
7500 Security Boulevard, Mail Stop N3-13-27
Baltimore, Maryland 21244-1850

OFFICE OF INFORMATION SERVICES

CIO DIRECTIVE 12-01

DATE: March 29, 2012

TO: CMS Center and Office Directors
Consortia Administrators

FROM: Tony Trenkle
CMS Chief Information Officer (CIO) and
Director, Office of Information Services (OIS)

SUBJECT: CIO Directive 12-01 – CMS Vulnerability Assessment and Penetration Testing – **ACTION**

Background

Under the *Federal Information Security Management Act of 2002* (FISMA), the Office of Management and Budget (OMB) directed the National Institute of Standards and Technology (NIST) to develop specific guidance for federal agencies to test and assess the security of their information systems. Additionally, network vulnerability assessment and penetration testing of information systems are procedures recommended in the Security Management and Access Controls portions of the Government Accountability Office (GAO) guidance provided in the *Federal Information System Controls Audit Manual* (FISCAM). NIST Special Publication (SP) 800-115, *Technical Guide to Information Security Testing and Assessment,* provides specific guidance for conducting these tests and assessments.

A vulnerability assessment is the systematic examination of an information system or product intended to accomplish the following objectives:

- Determine whether or not security controls are adequately designed and effectively implemented;
- Identify security deficiencies and determine the effectiveness of external perimeter and internal security controls;
- Provide a basis for evaluating the effectiveness of proposed or implemented security measures;
- Map the vulnerabilities with associated exploits; and
- Confirm post-implementation of changes made to security baseline and other protective measures.

Penetration testing is security testing in which assessors simulate real-world attacks to identify vulnerabilities in security features of an application, system, or network or operational weaknesses in process or technical countermeasures. It often involves launching attacks on production systems along with using tools and techniques commonly used by attackers. Most penetration tests involve looking for combinations of vulnerabilities on one or more systems that can be used to gain more access than could be achieved through a single vulnerability. Penetration testing can also be useful for determining:

1. How well the system tolerates real world-style attack patterns;
2. The likely level of sophistication an attacker needs to successfully compromise the system;
3. Additional countermeasures that could mitigate threats against the system; and
4. Defenders' ability to detect attacks and respond appropriately.

Purpose

The primary goal of the CMS Vulnerability Assessment and Penetration Testing Program is to continuously test and assess the security of all CMS information systems. As it is already defined and therefore required within the *CMS Acceptable Risk Safeguards*, vulnerability assessments and penetration testing are required in order to not only meet FISMA and other regulatory standards, but to also ensure that CMS assets are protected against the ever growing worldwide cybersecurity threats.

As part of this initiative, the CMS vulnerability assessment and penetration testing program will facilitate standard and effective information security vulnerability data collection and dissemination. The scope of the assessment and testing activities will include both Federal and contractor operated data centers. The output of these activities will provide the CMS senior management and CMS Business Owners with vulnerability information specific to individual FISMA systems, as well as across the CMS enterprise (as applicable), that is consistent, measureable, accurate, and current.

Implementation

The CMS Office of the Chief Information Security Officer (OCISO) has engaged the services of several contractors to help implement this program. The contractors, along with Federal OCISO staff, have been tasked to conduct vulnerability assessment and penetration testing on CMS FISMA systems and networks, in a systematic and repeatable fashion. The OCISO will be establishing automated testing capabilities, as well as manual processes for conducting vulnerability assessment and penetration testing.

To ensure the protection of sensitive information collected during testing, OCISO and their contractors will utilize the necessary controls to protect this information. These controls include, but are not limited to the following:

- Non-disclosure arrangements that are all inclusive of OCISO contractor interactions with CMS and their interactions with entities that perform work on behalf of CMS;
- Stringent requirements on sensitive information handling;

- FISMA authorized to operate facilities to store, process, and transmit sensitive information; and
- Close supervision by OCISO Federal employees.

As part of the ongoing outreach and data collection process, CMS Business Owners, System Developer and Maintainers, and/or their support contractors may be asked to provide additional information and coordination in the following information security related areas in order to better facilitate testing:

- Vulnerability Management;
- Configuration Management;
- Boundary Protection;
- Patch Management;
- Identity and Access Management;
- Incident Management;
- Network Security Protocols; and
- Data Protection.

The CMS CIO will sign, on behalf of all CMS Business Owners, a Rules of Engagement (ROE). This document contains the information specified in NIST SP 800-115 and will establish the detailed guidelines for conducting the testing that will be used to evaluate CMS FISMA systems. The ROE gives the test team authority to conduct defined activities without the need for additional permissions. OCISO personnel will coordinate with the CMS Business Owners and their designated representatives to ensure that the testing schedule and scope is understood.

Vulnerabilities discovered during a vulnerability assessment or penetration test will be assigned to the appropriate CMS Business Owner for remediation and placed in the CMS FISMA Controls Tracking System (CFACTS) following the established CMS Plan of Action and Milestone (POA&M) process.

Timeframe

The CMS OCISO has started to contact various CMS Business Owners to coordinate vulnerability assessment and penetration testing schedules. Subsequent vulnerability assessment and penetration testing activities will continue throughout the operational life of CMS FISMA systems.

Direction

OCISO will work with CMS Business Owners, System Developers and Maintainers, Information System Security Officers, and their contractors to:

- Identify corrective actions needed to remediate vulnerabilities;

- Identify areas and methods for improvement; and
- Provide timely reports on testing activities and results.

This memorandum requires and authorizes CMS Business Owners, System Developers and Maintainers, Information System Security Officers, and their contractors to allow the CMS OCISO to conduct vulnerability assessments and penetration testing throughout the operational life of CMS FISMA systems in accordance with the Rules of Engagement agreed upon. CMS Business Owners, System Developers and Maintainers, Information System Security Officers, and their contractors are also required and authorized to release sensitive system or network-related information to OCISO for the purpose of supporting the vulnerability assessment and penetration testing activities.

Contacts

If you have questions or require additional information on this directive, the Office of the Chief Information Security Officer team is available to support staff level questions at CISO@cms.hhs.gov.

/s/
Tony Trenkle
CIO and Director, OIS

cc:
Distribution